Amendments to the Title

Please replace the Title with the following marked-up replacement Title:

-- Method, System, and Computer Program Product for Generating Pseudo-Random Bits --

Amendments to the Specification

Please replace the paragraph that begins on Page 8, line 13 and carries over to Page 9, line 2 with the following marked-up replacement paragraph:

-- In a preferred embodiment, the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption. In one aspect, the 1-way function is modular exponentiation modulo a safe prime number. In this aspect, the input value is used as an exponent of the modular exponentiation. Furthermore, a base of the modular exponentiation is a fixed generator value. Preferably, the length of the input value is 160 bits and a length of the safe prime number is 1024 bits. Alternatively, the lengths maybe greater than or equal to 160 and 1024, respectively. The length of the generated output sequence is also preferably 1024 bits, but may alternatively by greater than 1024 bits (and in either case, is identical to the length of the safe prime number.) --